УДК 343

АКТУАЛЬНОСТЬ СОВЕРШЕНСТВОВАНИЯ ОТДЕЛЬНЫХ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ И УГОЛОВНЫХ НОРМ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Д. В. Свешников
Могилевский институт МВД Республики Беларусь,
курсант 4 курса факультета милиции

Ж. А. Шилко
Могилевский институт МВД Республики Беларусь,
старший преподаватель кафедры
уголовного процесса и криминалистики
e-mail: shilko.zhanna@mail.ru

Аннотация. *В статье рассматриваются пробелы в действующем уголовном и уголовно-процессуальном законодательстве, не позволяющие эффективно противодействовать отдельным киберпреступлениям; аргументируется необходимость совершенствования соответствующих правовых норм.*

Ключевые слова: *компьютерная информация, несанкционированный доступ, хищение денежных средств, банковская карта.*

Annotation. *The article discusses the gaps in the current criminal and criminal procedural legislation, which do not allow to effectively counteract certain cybercrimes, and the need to improve the relevant legal norms is argued.*

Keywords: *computer information, unauthorized access, embezzlement of funds, bank card.*

Общедоступность информационных технологий для их использования гражданами, не обладающими достаточными познаниями в сфере информационной безопасности, все более широкое распространение банковских платежных карт и увеличение доли безналичных средств в денежном обороте, развитые сетевые инструменты для анонимизации, высокая латентность, а также возможность совершения деяний из любой точки земного шара делают киберпреступления все более распространенными. С каждым годом преступления данного вида составляют все больший удельный вес среди возбужденных уголовных дел как в Республике Беларусь, так и во всем мире.

С целью выявления и пресечения такого рода преступлений Министерством внутренних дел Республики Беларусь около двух десятилетий назад созданы подразделения по раскрытию преступлений в сфере высоких технологий, в настоящее время переименованные в подразделения по противодействию киберпреступности. Стремительный ежегодный рост количества преступлений в данной сфере подтверждает необходимость и важность их существования.

Однако принятие одних лишь организационно-штатных мер без соответствующего законодательного совершенствования не позволит снизить количество противоправных действий и эффективно противостоять киберпреступности.

Уголовное законодательство Республики Беларусь, как и многих других государств, устанавливает ответственность за общественно опасные деяния, связанные с компьютерной техникой. Так, ответственность за хищение денежных средств с использованием компьютерной техники предусмотрена статьей 212 Уголовного кодекса Республики Беларусь (далее — УК) [1]. Под хищением путем использования компьютерной техники в данной норме следует понимать незаконное завладение имуществом путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации. Стоит отметить, что в отличие от иных преступлений против собственности, таких как хищение имущества путем кражи, мошенничества, злоупотребления служебными полномочиями, присвоения или растраты, в статье 212 УК не обозначается минимальный размер имущественного вреда для привлечения к уголовной ответственности, а административная ответственность за такие противоправные действия не предусмотрена вовсе.

Практика показывает, что данный пробел в законодательстве весьма актуален, поскольку как хищение путем использования компьютерной техники квалифицируется и несанкционированная оплата либо снятие денежных средств в банкомате с использованием утерянной банковской платежной карты. Однако государственные затраты на уголовное преследование и реализацию мер уголовного наказания в таких случаях не соразмерны с общественной опасностью этих деяний. В связи с этим, представляется целесообразным и своевременным дополнить перечень преступлений, имеющийся в части 4 примечания к 24-й главе УК, при совершении которых лицо не подлежит уголовной ответственности, хищением имущества физического путем использования компьютерной техники лица в сумме, не превышающей двух базовых величин.

При хищении имущества юридического лица в сумме, не превышающей десяти базовых величин, необходимость введения аналогичного подхода отсутствует, поскольку на имя юридических лиц банковские платежные карты не эмитируются.

Стоит отметить, что хищение самой банковской платежной карты состава преступления либо административного правонарушения не образует, так как банковская платежная карта не имеет стоимости. Вместе с тем фактическое исчезновение и компрометация банковской карты [2] влекут за собой временные и финансовые потери лица, на которого она эмитирована, в том числе по ее перевыпуску. В связи с этим представляется целесообразным введение админи-

стративной ответственности за умышленное хищение банковской платежной карты при наличии требования ее владельца.

Кроме этого, в целях совершенствования действующего уголовного законодательства и унификации правоприменительной практики существует необходимость переработки содержания статьи 212 УК. В связи с тем, что несанкционированная оплата банковскими платежными картами другого лица всегда сопряжена с несанкционированным доступом к компьютерной информации, первая часть данной уголовной нормы для квалификации деяний на практике применяется крайне редко. Таким образом, данную норму, отраженную в части 1 статьи 212 УК, в связи с невысокой степенью общественной опасности деяния предлагается декриминализовать и вынести в отдельную норму административного законодательства с соответствующим смягчением санкции: *«Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации».*

Вместе с тем факт совершения несанкционированных операций в сети Интернет должен являться квалифицирующим признаком хищения с использованием компьютерной техники, так как действия, совершенные с использованием физической карты, и действия, совершенные в сети Интернет, фактически отличаются общественной опасностью деяний. Предлагаем статью 212 УК изложить в следующей редакции:

«1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к компьютерной информации —

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо с использованием глобальной компьютерной сети Интернет —

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, —

наказываются лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, —

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения».

Продолжая наше рассуждение в контексте назревших нормативных изменений, напомним, что частью 6 Примечания к главе 24 УК («Преступления против собственности») установлено, что уголовное преследование близких потерпевшего, совершивших кражу путем использования компьютерной техники (часть 1 статьи 212), возбуждается только по заявлению потерпевшего, а в случае его неспособности по возрасту или состоянию здоровья выражать свою волю в уголовном процессе либо в случае его смерти — любого из его совершеннолетних близких родственников или членов семьи, его законного представителя. Как показывает анализ практической деятельности, нередко имеют место случаи хищения денежных средств с банковских платежных карт близкими родственниками, в том числе несовершеннолетними детьми у родителей, путем привязки банковских карт к различным сервисам в сети Интернет. После установления таких фактов заявитель, разумеется, категорически отказывается привлекать близкого родственника к уголовной ответственности. То есть в настоящее время имеет смысл и практическая необходимость добавить к части 1 статьи 212 УК и часть 2. Соответствующие изменения необходимо внести и в часть 3 статьи 26 Уголовно-процессуального кодекса Республики Беларусь, определяющую категории уголовных дел, относящихся к частному обвинению [3].

Также, по нашему мнению, белорусскому законодателю следует четко определить, при каких условиях имеет место повторность деяния по статье 212 УК, в связи с тем что в настоящее время в следственных подразделениях Республики Беларусь нет единообразного подхода по квалификации повторности деяний по данной статье. Позиция отдельных следственных подразделений состоит в том, что каждая операция, совершенная в одной торговой точке с разницей во времени в одну или несколько минут, представляет собой результат нового преступного умысла. Для других подразделений единый преступный умысел хищения средств с банковских платежных карт охватывает все операции с использованием данной карты, даже если операции совершены в различ-

ных торговых точках с разницей в несколько дней. В настоящее время к данной проблемной ситуации требуется аналитический подход как со стороны суда, так и органов прокуратуры с целью обобщения подобных случаев, единообразного толкования уголовных норм и выработки единой правоприменительной практики. В настоящий момент данной проблеме не уделяется достаточного внимания, в том числе в связи с тем, что разные подходы не влияют на квалификацию инкриминируемой статьи (часть 2 статьи 212 УК), поскольку квалифицирующий признак повторности содержится в данной части наряду с несанкционированным доступом к компьютерной информации.

Таким образом, предлагаемые в настоящей публикации изменения и дополнения в действующее уголовное и уголовно-процессуальное законодательство Республики Беларусь являются необходимостью, продиктованной практической деятельностью органов, осуществляющих уголовное преследование лиц, совершающих киберпреступления. Глубокая законодательная проработка обозначенных проблемных вопросов позволит определить вектор для их последующего разрешения.

---

1. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : с изм. и доп. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

2. Компрометация карточки [Электронный ресурс] // Официальный сайт Беларусбанка. URL: https://belarusbank.by/ru/33139/press/finansovaya-gramotnost/terminy/komprometaciya_kartochki/ (дата обращения: 28.02.2021). Перейти к источнику Вернуться к статье

3. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : с изм. и доп. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье